

Remarks

Status of the Claims

Claims 23-29, 31-41, 43-45 and 56-57 were pending in the application and stand rejected. By this paper, claims 29, 31-41, 44-45 and 56-57 have been amended, claims 58-60 have been added, and claims 23-28 have been canceled without prejudice or disclaimer. For the reasons set forth below, Applicant submits that each of the pending claims is patentably distinct from the cited prior art and in condition for allowance. Reconsideration of the claims is therefore respectfully requested.

Interview Summary

Applicant would like to thank Examiner Moorthy for the interview extended to Applicant's attorneys, Kory D. Christensen and Aaron D. Barker, on December 9, 2006. During the interview, Applicant discussed U.S. Patent No. 6,195,751 to Caronni et al. ("Caronni") and clarified patentably distinguishing features of the invention. Pending a further search by the Examiner, an agreement was reached relating to claim language. Accordingly, Applicant has amended the claims along the lines discussed in the interview. Further, per the Examiner's suggestion in the interview, Applicant has canceled claims 23-28 without prejudice or disclaimer. Therefore, Applicant respectfully requests reconsideration of the pending amended claims.

35 U.S.C. § 101

Claims 29 and 31-40 were rejected under 35 U.S.C. § 101 as being allegedly directed to non-statutory subject matter because the present specification recites a machine-readable medium that may include a propagation media. Accordingly, Applicant has amended claims 29 and 31-40 to recite, among other things, a "machine-readable **storage** medium." The additional word "storage" is meant to include all types of data storage devices, both volatile and non-volatile. The present specification gives examples of physical storage mediums such as "floppy diskettes, optical disks, CD-ROMs, and magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnet or optical cards." Page 43, lines 18-19. Applicant submits that such a program product is statutory subject matter and excludes non-physical media such as signals or other types of propagation media. Thus, Applicant respectfully requests that the rejection under 35 U.S.C. § 101 be withdrawn.

35 U.S.C. § 102

Claims 23-29, 31, 32, 36-41, 43, 44, and 56-57 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,195,751 to Caronni et al. ("Caronni"). However, Applicant respectfully traverses this rejection because Caronni fails to identically teach every element of the claims. See M.P.E.P. § 2131 (stating that in order to anticipate a claim, a prior art reference must identically teach every element of the claim).

Claim 29, as amended herein recites, among other things:

encrypting a first group of unencrypted multimedia channels
using conditional access ("CA") encryption to produce a first group of
encrypted multimedia channels;

encrypting said first group of unencrypted multimedia channels
using a different type of encryption to produce a second group
of encrypted multimedia channels; and\

***simulcasting said first group of encrypted multimedia channels
simultaneously with said second group of encrypted multimedia
channels to a plurality of multimedia subscribers....***

New multimedia receivers may use advanced types of encryption as compared to legacy multimedia receivers. The different types of encryption are not interchangeable. For example, the legacy multimedia receivers cannot decrypt the more advanced types of encryption that the new multimedia receivers are able to decrypt.

According to the claimed invention, the ***same, original*** first group of unencrypted multimedia channels is encrypted using *two different types of encryption*. Thus, after encryption, the two encrypted groups are two versions of the same multimedia content. Each version includes the content of the first group of multimedia channels, but with a different encryption. The two versions are then ***broadcast simultaneously*** (e.g., simulcast) to subscribers. For example, Figure 16 (reproduced below) of the present application shows two versions of "premium" digital channels being broadcast at the same time. A first version (see element 1626) is encrypted using standard encryption, and a second version (see element 1628) is encrypted using alternate encryption.

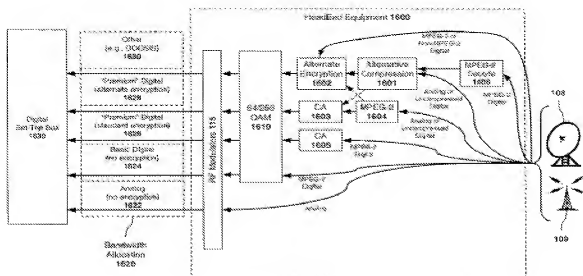
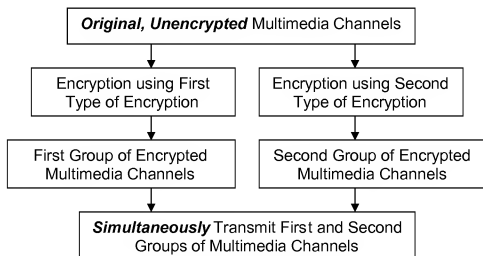


FIG. 16

As shown in the drawing below, the claims provide a parallel process that encrypts original, unencrypted multimedia channels two times using two different types of encryption so that two viewers, using different types of receivers, can view the same program at the same time.



By way of contrast with the pending claims, Caronni does not teach or suggest encrypting the same, **original** channel twice and then transmitting the encrypted channels at the same time. Rather, Caronni teaches increasing the security of group messages by changing encryption keys when participants join or leave an authorized group. Col. 2, lines 22-24, and 62-66.

Caronni teaches securing communications by using two different types of encryption keys. The first key is called a traffic encryption key (TEK) that is used to encrypt and decrypt messages sent between all participants in the group. Col. 8, lines 50-57. The second type of key is called a key encryption key (KEK). As the name suggests, KEKs are used to encrypt the keys sent between the participants in the group. Each of the participants knows a unique set of KEKs that overlap with a portion of the KEKs known by other users (virtual subgroups). The purpose of the virtual subgroups of common KEKs is to allow controlled distribution of encryption keys. Thus, when a particular participant leaves the group, another participant can generate a new TEK, throw out the KEKs known to the leaving participant, and distribute the new TEK to the remaining participants using the remaining KEKs. Col. 14, lines 47-67.

However, Caronni is silent as to the subject matter of the pending claims. The portion of Caronni cited by the Office Action (col. 7, line 46 to col. 8, line 20) does not address simultaneously transmitting a message encrypted with different keys. Rather, it deals with two completely different embodiments that do not imply any simultaneous action between the two embodiments. The portion cited at col. 7, lines 46-58 corresponds to a distributed implementation shown in FIG. 1a wherein the

keys are stored in a flat data structure that is distributed across multiple participants. See col. 6, lines 4-8, and 60-61. The portion cited at col. 7, line 59 to col. 8, line 20 corresponds to an alternate implementation shown in FIG. 1b wherein the keys are stored in a flat data structure implemented in a centralized entity. See col. 6, lines 32-36, and 62. Applicants respectfully submit that Caronni does not teach or suggest that the two different implementations shown in FIGs. 1a and 1b are used at the same time to simultaneously transmit the same messages using two different types of encryption.

In view of the foregoing, all pending claims represent patentable subject matter. A Notice of Allowance is respectfully requested.

Respectfully submitted,

Digeo, Inc.

By /Kory D. Christensen/
Kory D. Christensen
Registration No. 43,548

STOEL RIVES LLP
One Utah Center Suite 1100
201 S Main Street
Salt Lake City, UT 84111-4904
Telephone: (801) 328-3131
Facsimile: (801) 578-6999